UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,635	06/30/2003	Jeffrey A. Aaron	60027.5044US01/BLS 030081	1408

7590 06/14/2007

Jodi L. Hartman
Hope Baldauff Hartman, LLC
1720 Peachtree Street, N.W., Suite 1010
Atlanta, GA 30309

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
06/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/611,635	AARON, JEFFREY A.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-39,41-43 and 45-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-39,41-43 and 45-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on March 22, 2007. Claims 9, 40 and 44 are canceled. Claims 1-8, 10-16, 19-31, 34-39, 41-43, 45, and 47 are amended. Further, new claims 48-53 are added. Thus claims 1-8, 10-39, 41-43, and 45-53 are pending/examined.

2. In the previous office action, Examiner objected claims 14-15, 29-30, and 46-47 as being dependent upon a rejected base claim, but indicated that these objected claims would be allowable if rewritten in independent form including all of the recitations of the base claims and any intervening claims. However, after further search and consideration the objection is withdrawn and this office action is made another non-final office action.

Response to Arguments

3. Applicant's remarks/arguments filed on March 22, 2007, regarding claims 1-8, 10-39, 41-43, 45-47 have been fully considered but they are not persuasive.

Applicant argument is based on the reference used in rejecting the corresponding limitation recited in the independent claims. Applicant argued that some of the limitation recited in the independent claim is not disclosed or taught by the reference on the record namely "**Cisco**".

Applicant wrote the following in support of his argument.

"Cisco does not teach, suggest, or describe a system for providing network-based firewall policy configuration and facilitation associated with a firewall as recited by claim 1. On the contrary, Cisco describes a firewall (Cisco Centri Firewall) operative to filter session attempts by evaluating the incoming request to start a new session against session controls and responses defined by a security policy to determine whether to allow the new session. Cisco further describes that the session controls used by the firewall to

determine whether to allow a new session may be run-time session controls which are session controls that can be modified at the time the session request is received by the firewall.

This is not analogous to the system recited by claim 1 because Cisco fails to teach, suggest, or describe that the firewall is operative to determine whether the new session includes one or more questionable packets and to modify the security policy to allow at least a portion of the packets associated with the new session to pass through the firewall unblocked, where the portion of the packets allowed is determined based on whether the new session includes one or more questionable packets. Instead, Cisco describes that the firewall is operative to use session controls that can be modified at the time the session request is received by the firewall to determine whether to allow the new session as a whole; without teaching or suggesting that the firewall is operative to determine whether the new session includes one or more questionable packets and to modify the security policy to allow at least a portion of the packets of the new session, where the portion of the packets allowed is based on whether or not the new session includes questionable packets."

Examiner disagrees with the above argument.

Examiner would point out that, on page 9, Cisco discloses, how the Cisco Centri Firewall enforces security polices, identifies and defines the major components of the architecture, and explains how it prevents common attacks through detailed evaluation of network packets and intelligent countermeasures, meets the limitation recited as "determine whether the application includes one or more questionable packets."

For instance applicant's published specification on paragraph 0048 discloses the following in support of this amendment.

"If the blocking history is completely acceptable i.e., the PMA finds no questionable packets, at 520, the user's firewall policy is modified by adding new rules allowing the passage of the new application's packet types to the set of firewall policy rules. Optionally

in some cases, it may be possible to ***modify existing rules rather than adding new rules, depending on the specifics of the rules and their parameters. The firewall policy rules are preferably formed from the pertinent aspects of the identified packets, such as the source and destination addresses, source and destination ports numbers, whether TCP or UDP packets, or other protocol numbers, etc"***

The reference on the record also discloses the same concept. For instance, Cisco on page 3, third paragraph discloses, that Centri Firewall filters session attempts according to the rules defined in a security policy. A security policy specifies which network objects are allowed to communicate with each other, and each security policy is designed to enforce some part of the overall network security policy defined by an organization. You can specify which internal network objects can communicate with which external network objects and vice versa. Other options exist by which you can filter communications, such as time of day, destination, and type of protocol being used to conduct the communication.

Furthermore, Cisco on page 3, paragraph 6 and 7, discloses Session control and ***Run-time session controls*** which are capable of determining whether the application includes one or more questionable packets at the run time.

"For instance, Under the session control, the following has been disclosed.
"Session controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static and *Run-time session controls* are those session controls that can be **modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service.**" And this meets the limitation recited as "to modify the user's firewall policy to allow at least a portion of the packets

associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets."

Therefore all limitations recited in the amended independent claims 1, 16 and 31 are undoubtedly disclosed by the reference/s on the record and the rejection is maintained until the applicant amends the body of the independent claims with further clarification and successfully overcome the rejection without introducing new matters.

The last argument presented by the applicant is towards the dependent claims which depend on the above independent claims.

Examiner disagrees with the argument as the dependent claims stands and falls with the corresponding independent claims.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. **Claims 1-8, 10-15, 31-39, 41-43, 45-49 and 52-53 are** rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.

6. **Claims 1-8, 10-15 and 48-49** are directed **to a system for providing network-based firewall policy configuration and facilitation associated with the firewall.** The examiner asserts that the limitation of the claim raises a question as to whether

such system claims are software as it recited on applicant's publication paragraph 0040, "...these modules are **software process, modules or routines.**" Furthermore on applicant's publication paragraph 0003, the firewall is recited as software firewalls. Likewise, examiner asserts that all elements in the body of the claims are programs /software and do not contain for instance processor or a hardware that will make the claim statutory.

These system claims do not clearly establish a statutory category of the invention. Therefore the claims are software/program per se and do not fall within the statutory classes listed in 35 USC 101. The language of the claims raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP § 2106 IV. B. 1(a).

7. **Claims 31-39, 41-43 and 45-47 and 52-53** are directed **to a computer-readable medium for providing network-based firewall police configuration and facilitation associated with a firewall.**

The examiner asserts that the limitation of the claim raises a question as to whether such computer-readable medium are appropriate medium that fall within the statutory classes listed in 35 USC 101.

However, as it is disclosed on applicant's publication paragraph 0026, the computer-readable medium could even **be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance optical scanning of the paper or other medium**. On the same paragraph such computer-readable medium can also be any means that can, **propagate** or **infrared or propagation medium.**

These computer-readable medium do not clearly establish a statutory category of the invention and do not fall within the statutory classes listed in 35 USC 101. The language of the claims raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP § 2106 IV. B. 1(a).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

9. **Claims 1-8, 10-13, 16-28, 31-39, 41-43 and 45** are rejected under 35 U.S.C. 102(a) as being anticipated by **an article written with the title "Understanding Security Policies"** (hereinafter referred as **Cisco**)(Publication date: September 28, 2002) (See reference U)

10. As per independent claims 1, 16 and 31 Cisco discloses a system for providing network-based firewall policy configuration and facilitation, comprising:

- **A firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user's firewall policy** *[See page 3, paragraph 5-7] ("By By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Session*

controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service and this run-time session controls meets adding an application not currently supported by a user's firewall policy.) and

- **To generate a time window during which a user can run the application**; *[See table 4-1 on page 3 and 4, see common Run-time controls] (These session controls are common to all network services. They define the basic elements of any session, such as* ***its time of day,*** *date, User ID, Host ID, and type of service. These controls are defined using security policies.) and*

- **A policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a firewall modification request from the firewall facilitation coordinator [***See page 3, paragraph 5-7 and see also table 4-1 on page 3 and 4, see common Run-time controls] (By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service. These session controls are common to all network services. They define the basic elements of any session, such as its time of day, date, User ID, Host ID, and type of service. These controls are defined using security policies)*

determine whether the application includes one or more questionable packets, [See page 9](*On page 9 Cisco discloses, how the Cisco Centri Firewall enforces security polices, identifies and defines the major components of the architecture, and explains how* ***it prevents common attacks through detailed evaluation of network packets and intelligent countermeasures****, meets the limitation recited as "determine whether the application includes one or more questionable packets." Because if the firewall has the capability of preventing common attacks through detailed evaluation of network packets and intelligent countermeasures then it implies that it has also the capability of determining whether the application includes one or more questionable packets/ attacking packets)* **and**

to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets. [Page 3, third paragraph and page 3, 6-7 paragraph] *(For instance applicant's published specification on paragraph 0048 discloses the following in support of this limitation. "If the blocking history is completely acceptable i.e., the PMA finds no questionable packets, at 520, the user's firewall policy* ***is modified by adding new rules allowing the passage of the new application's packet types to the set of firewall policy rules. Optionally in some cases, it may be possible to modify existing rules rather than adding new rules, depending on the specifics of the rules and their parameters. The firewall policy rules are preferably formed from the pertinent aspects of the identified packets, such as the source and destination addresses, source and destination ports numbers, whether TCP or UDP packets, or other protocol numbers, etc."*** *The reference on the record also discloses the same concept. For instance, Cisco on page 3, third paragraph discloses, that Centri Firewall filters*

session attempts according to the rules defined in a security policy. A security policy specifies which network objects are allowed to communicate with each other, and each security policy is designed to enforce some part of the overall network security policy defined by an organization. You can specify which internal network objects can communicate with which external network objects and vice versa. Other options exist by which you can filter communications, ***such as time of day, destination, and type of protocol being used to conduct the communication.*** *Furthermore, Cisco on page 3, paragraph 6 and 7, discloses Session control and* Run-time session controls *which are capable of determining whether the application includes one or more questionable packets at the run time. For instance, under the session control, the following has been disclosed.* "Session controls are predominately specific to a network service and are used to act upon a session to provide strict*er control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static and* Run-time session controls ***are those session controls that can be modified at the time the session request is received by the firewall.*** *Run-time session* ***controls are defined using security policies and can either apply to all communications or to a specific network service."*** *And this meets the limitation recited as "to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets.")*

11. <u>As per claims 2-8, 10-13, 17-28, 32-39, 41-43 and 45</u> Cisco discloses a system/method as applied to claims above. Furthermore Cisco discloses the method/system, further comprises a firewall process adapted to communicate with the policy modification agent, the firewall process includes the user's firewall policy, a firewall communications or packet inspector and a firewall filter. *[See*

page 3, Paragraph 3 and See page 3, paragraph 5-7 and see also table 4-1 on page 3 and 4, see common Run-time controls](Similarly, Cisco Centri Firewall filters session attempts according to the rules defined in a security policy. A security policy specifies which network objects are allowed to communicate with each other, and each security policy is designed to enforce some part of the overall network security policy defined by an organization. You can specify which internal network objects can communicate with which external network objects and vice versa. Other options exist by which you can filter communications, such as time of day, destination, and type of protocol being used to conduct the communication. (By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session.Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service. These session controls are common to all network services. They define the basic elements of any session, such as its time of day, date, User ID, Host ID, and type of service. These controls are defined using security policies)

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. **Claims 14-15, 29-30, 46-53** are rejected under 35 U.S.C. 103(a) as being unpatentable over **an article written with the title "Understanding Security**

Policies" (hereinafter referred as **Cisco**)(Publication date: September 28, 2002) (See reference U, previously submitted) in view of **Yoshihara et al** (hereinafter referred as **Yoshihara**)(U.S. Patent Publication No. 2002/0040396 A1) (filed on September 27/2001)

14. As per claims 14-15, 29-30, 46-53 Cisco discloses a system for providing network-based firewall policy configuration and facilitation, comprising:

- **A firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user's firewall policy** *[See page 3, paragraph 5-7] ("By By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Session controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service and this run-time session controls meets adding an application not currently supported by a user's firewall policy.) and*

- **To generate a time window during which a user can run the application**; *[See table 4-1 on page 3 and 4, see common Run-time controls] (These session controls are common to all network services. They define the basic elements of any session, such as* ***its time of day,*** *date, User ID, Host ID, and type of service. These controls are defined using security policies.) and*

- **A policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a**

firewall modification request from the firewall facilitation coordinator [*See page 3, paragraph 5-7 and see also table 4-1 on page 3 and 4, see common Run-time controls*] *(By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service. These session controls are common to all network services. They define the basic elements of any session, such as its time of day, date, User ID, Host ID, and type of service. These controls are defined using security policies)*

determine whether the application includes one or more questionable packets, [See page 9](*On page 9 Cisco discloses, how the Cisco Centri Firewall enforces security polices, identifies and defines the major components of the architecture, and explains how* ***it prevents common attacks through detailed evaluation of network packets and intelligent countermeasures****, meets the limitation recited as "determine whether the application includes one or more questionable packets." Because if the firewall has the capability of preventing common attacks through detailed evaluation of network packets and intelligent countermeasures then it implies that it has also the capability of determining whether the application includes one or more questionable packets/attacking packets)* **and**

to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets. [Page 3,

third paragraph and page 3, 6-7 paragraph] *(For instance applicant's published specification on paragraph 0048 discloses the following in support of this limitation. "If the blocking history is completely acceptable i.e., the PMA finds no questionable packets, at 520, the user's firewall policy* ***is modified by adding new rules allowing the passage of the new application's packet types to the set of firewall policy rules. Optionally in some cases, it may be possible to modify existing rules rather than adding new rules, depending on the specifics of the rules and their parameters. The firewall policy rules are preferably formed from the pertinent aspects of the identified packets, such as the source and destination addresses, source and destination ports numbers, whether TCP or UDP packets, or other protocol numbers, etc."*** *The reference on the record also discloses the same concept. For instance, Cisco on page 3, third paragraph discloses, that Centri Firewall filters session attempts according to the rules defined in a security policy. A security policy specifies which network objects are allowed to communicate with each other, and each security policy is designed to enforce some part of the overall network security policy defined by an organization. You can specify which internal network objects can communicate with which external network objects and vice versa. Other options exist by which you can filter communications,* ***such as time of day, destination, and type of protocol being used to conduct the communication****. Furthermore, Cisco on page 3, paragraph 6 and 7, discloses Session control and* Run-time session controls *which are capable of determining whether the application includes one or more questionable packets at the run time. For instance, under the session control, the following has been disclosed.* "Session controls are predominately specific to a network service and are used to act upon a session to provide strict*er control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static and* Run-time session controls ***are those session controls that can be modified at the time the session request is received by the firewall.*** *Run-time*

session ***controls are defined using security policies and can either apply to all communications or to a specific network service."*** *And this meets the limitation recited as "to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets.")*

Cisco does not explicitly teach wherein the policy modification agent is further configured to group the types of questionable packets singly and in combination of two or more, and to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

However, in the same field of endeavor, **Yoshihara on paragraph 0034 discloses the following,**

"Counters 3113 to 3117 count the number of passing IP packets or the number of IP packet bytes. An unconditional dropper 3107 discards a packet unconditionally. Selective droppers 3108, 3109, and 3110 **discards selectively a packet under a predetermined condition**. Queues 3118 to 3121 queue an input IP packet. A scheduler 3130 reads out packets from such queues 3118 to 3121 **each in accordance with a predetermined sequence and priority,** and outputs them to an output I/F 36." Furthermore, on paragraph 0100, Yoshihara discloses the following, "the present invention is similarly applicable **to policy based network management employing a firewall for making customized access control for each user, company, host, terminal, and application**" and this meets the limitation recited as, "the policy modification agent is further configured to group the types **of questionable packets** singly and in combination of two or more, and **to prioritize** the groups based on a likelihood that the groups **will be required to be added to the firewall policy** in order

to allow the new application to function properly, and to label **the groups in order of priority.**"

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of prioritizing the groups based on a likelihood that the groups **will be required to be added to the firewall policy** in order to allow the new application to function properly, and to label **the groups in order of priority** as per teachings of **Yoshihara** in to the method of run time policy modification as taught by **Cisco** for the purpose of dynamically adjust the policy based on priority.[See for instance, **Yoshihara's abstract]**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
06/01/2007

Benjamin E Lanier
Examiner AU 2132